

CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1, 2, 6-9, 11, 22-24, 28, 31, 32, 43, 46 and 47.
- After this Amendment: Claims 1, 2, 6-9, 11, 22-24, 28, 31, 32, 43, 46-47, and 49.

Non-Elected, Canceled, or Withdrawn claims: None

Amended claims: 2, 6, 22, 31, and 43

New claims: 49

Claims:

- 1. (Previously Presented)** A method comprising:
- generating a formal license for content that includes:
 - a decryption key for decrypting the content; and
 - access rules for accessing the content; and
 - configuring a plurality of license authorities to provide a plurality of partial licenses, wherein:
 - each said license authority provides a respective said partial license; and
 - the plurality of partial licenses are combinable to form the formal license;
 - wherein the configuring includes:
 - generating a pre-license from the formal license by encrypting the formal license utilizing an asymmetric encryption algorithm having a public key and a private key, wherein the formal license, the pre-license and the public key are denoted, respectively, as "license", "prel" and "PK" as follows:
$$\text{prel} = (\text{license})^{\text{pk}};$$
 - dividing the private key SK into m partial secret shares according to a (k, m) threshold secret sharing scheme by:
 - generating a sharing polynomial f(x) being represented as follows:
$$f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1} \quad , \text{ where } a_0 = \text{SK}; \text{ and}$$

calculating each said partial secret share, denoted as S_i , for a respective said license authority, denoted by id_i , in which $i = 1, \dots, m$, as follows:

$S_i = f(id_i) \bmod \phi(N)$, where N is a RSA modulus and $\phi(N)$ is a Euler totient function; and

transmitting the pre-license and a respective said partial secret share to a respective said license authority, wherein each said license authority is configured to generate the respective said partial license from the respective said partial secret share and the pre-license.

2. (Currently Amended) A method as described in claim 0, wherein the plurality of partial licenses ~~are~~ is provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

3-5. (Canceled)

6. (Currently Amended) A method as described in claim 1, wherein each said license authority verifies the pre-license and the respective said partial secret share by utilizing a verifiable secret sharing (VSS) scheme in which k public witnesses of the sharing polynomial's $f(x)$ coefficients (denoted as $\{g^{a_0}, \dots, g^{a_{k-1}}\}$, where $\underline{g \in Z_N}$ ~~$g \in Z_N^*$~~) are communicated to each said license authority id_i to verify validity of a respective said partial secret share S_i by determining if the following equation holds:

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \dots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N.$$

7. (Original) A method as described in claim 0, further comprising packaging the content to include one or more network addresses that are suitable for locating each said license authority.

8. (Original) A method as described in claim 0, wherein each said license authority is communicatively coupled to a peer-to-peer network.

9. (Original) A method as described in claim 0, wherein the plurality of license authorities are configured based on a consideration such that at least one said license authority provides two or more said partial licenses, wherein the consideration is selected from the group consisting of:

security of the at least one said license authority against unauthorized access;

load sharing of the plurality of license authorities;

availability of each said license authority;

network availability of each said license authority;

hardware resources of each said license authority;

software resources of each said license authority; and

any combination thereof.

10. (Canceled)

11. (Original) One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 0.

12-21. (Canceled)

22. (Currently Amended) A method comprising:

obtaining a plurality of partial licenses over a network from a plurality of license authorities, wherein each said partial license is provided, respectively, by a different said license authority; and

forming a formal license from the plurality of partial licenses, wherein the formal license includes access rules and a decryption key for accessing content, wherein:

the plurality of partial licenses are obtained from the plurality of license authorities by:

calculating the partial license $prel_i$ by each said license authority i from a partial secret share S_i and a pre-license $prel$ according to the following equation:

$$prel_i = (prel)^{S_i} \bmod N;$$

generating a random number u to calculate $A1 = gu$, $A2 = prelu$, $r = u - c * S_i$, and

$$c = \text{hash}(g^{S_i}, prel_i, A_1, A_2); \text{ and}$$

communicating the partial license $prel_i$, $A1$, $A2$, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by
validating each said partial license $prel_i$ by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \dots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N$$

from public witnesses of a sharing polynomial's coefficients, which
are denoted as $\{g^{a_0}, \dots, g^{a_{k-1}}\}$, that was utilized to generate the partial secret

share S_i , where $g \in Z_N$ ~~$g \in Z_N^*$~~ ,

applying $c = \text{hash}(g^{S_i}, prel_i, A_1, A_2)$ to calculate c ; and

checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial
license $prel_i$, and if so, each said partial license $prel_i$ is valid; and

combining the plurality of partial licenses to form the formal license,
denoted as $license$, when k valid said partial licenses are obtained, in
which:

$$\begin{aligned} license &= \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)} \\ &= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N, \end{aligned}$$

where

$$l_{id_i}(x) = \prod_{j=1, j \neq i}^k \frac{x - id_j}{id_i - id_j}.$$

23. (Original) A method as described in claim 0, wherein the obtaining includes:

examining the content to find a plurality of network addresses of a plurality of license authorities;

requesting the plurality of partial licenses from the plurality of license authorities; and

receiving one or more communications having one or more said partial licenses that are provided by each said license authority.

24. (Original) A method as described in claim 0, wherein the forming includes combining the plurality of partial licenses to form the formal license.

25-27. (Canceled)

28. (Original) One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 0.

29-30. (Canceled)

31. (Currently Amended) A method comprising:

configuring a plurality of license authorities in a first arrangement to provide a plurality of partial licenses, wherein:

each said license authority provides at least one said partial license; and

the plurality of partial licenses are combinable to form a formal license that includes access rules and a decryption key for content; and

updating the first arrangement to form a second arrangement such that:

each said license authority in the second arrangement provides at least one of a plurality of updated partial licenses that are combinable to form the formal license; and

the partial licenses provided in the first arrangement are not combinable with the updated partial licenses to form the formal license;

wherein the updating is performed by:

generating a random (k, m) sharing by each license authority i using a random update polynomial f_i , update(x), wherein:

$$f_{i,update}(x) = b_{i,1}x + \dots + b_{i,k-1}x^{k-1} \text{ mod } \phi(N);$$

and

distributing a subshare $S_{i,j}$ by each said license authority i such that each said license authority i has a respective said subshare $S_{i,j}$ from another said license authority wherein:

the subshare $S_{i,j} = f_{i,update}(j)$, $j = 1, \dots, m$ is calculated by each said license authority i;

the subshare $S_{i,j}$ is added to the original share S_i of each said license authority to form a new updated share

$$S'_i = S_i + \sum_{j=1}^m S_{j,i}; \text{ and}$$

a new secret sharing polynomial $f_{new}(x)$ is formed which is a summation of an original polynomial $f(x)$ utilized to generate the plurality of partial licenses in the first ~~arrange~~ arrangement and each of the randomly generated polynomials $f_{i,update}(x)$.

32. (Original) A method as described in claim 0, wherein the updating is performed periodically.

33-42. (Canceled)

43. (Currently Amended) A client device comprising:

a processor; and

memory configured to maintain:

packaged content that includes one or more network addresses that are suitable for locating a plurality of license authorities, wherein each said license authority stores one or more partial licenses;

a content player that is executable on the processor to output content; and

a digital rights management module that is executable on the processor to:

obtain the partial licenses from the plurality of license authorities utilizing the one or more network addresses; and

form a formal license from the obtained partial licenses, wherein the formal license provides access to the packaged content for output by the content player;

obtain the partial licenses from the plurality of license authorities, wherein each said license authority provide a respective said partial license by:

calculating the partial license pre_i by each said license authority i from a partial secret share S_i and a pre-license pre according to the following equation:

$$prel_i = (prel)^{S_i} \bmod N;$$

generating a random number u to calculate $A1 = gu$, $A2 =$

$prelu$, $r = u - c * Si$, and

$$c = hash(g^{S_i}, prel_i, A_1, A_2); \text{ and}$$

communicating the partial license $prel_i$, $A1$, $A2$, and r by each

said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by

validating each said partial license $prel_i$ by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \dots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \bmod N$$

from public witnesses of a sharing polynomial's

coefficients, which are denoted as $\{g^{a_0}, \dots, g^{a_{k-1}}\}$, that was

utilized to generate the partial secret share Si , where $\underline{g \in Z_N}$

$$\underline{g \in Z_N^*},$$

applying $c = hash(g^{S_i}, prel_i, A_1, A_2)$ to calculate c ; and

checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license $prel_i$, and if so, each said partial license $prel_i$ is valid; and

combining the plurality of partial licenses to form the formal license, denoted as license, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$

$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N,$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^k \frac{x - id_j}{id_i - id_j}.$

44-45 (Canceled).

46. (Original) A client device as described in claim 0, wherein the one or more network addresses include a proxy address for locating a network address of each said license authority.

47. (Original) A client device as described in claim 0, wherein the one or more network addresses include a network address of each said license

authority.

48. (Canceled)

49. (New) A method comprising:

receiving a formal license at a license authority from a content publisher, the formal license including a decryption key and access rules relating to particular content, wherein the access rules specify a plurality of time durations to access particular content based on respective payment amounts;

receiving a request at the license authority from a client device for a partial licenses related to the particular content;

sending a request from the license authority to the client device for additional information specifying an output duration to access the particular content;

generating the partial license at the license authority based on the formal license and a response received from the client device specifying the output duration; and

sending the partial license to the client device.